

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-136237

(43)Date of publication of application : 21.05.1999

(51)Int.Cl. H04L 12/24  
H04L 12/26  
H04L 12/46  
H04L 12/28

11-136237 U.S. PTO  
09/761696  
01/18/01

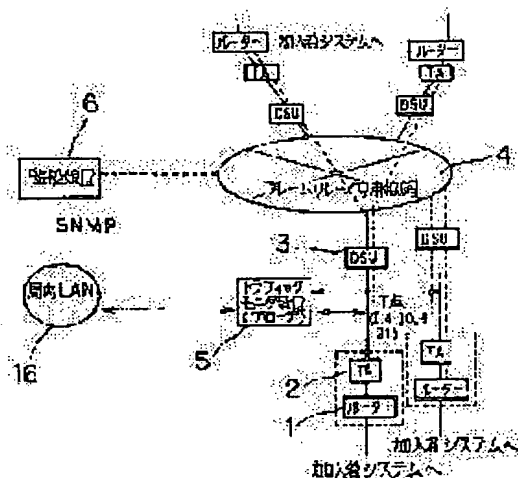
(21)Application number : 09-301068 (71)Applicant : NEC CORP  
(22)Date of filing : 31.10.1997 (72)Inventor : IWASAKI JUNKO

## (54) NETWORK TRAFFIC MONITOR SYSTEM

## (57)Abstract:

PROBLEM TO BE SOLVED: To provide the network traffic monitor system by which traffics suitable for a WAN are collected and monitored and where statistic information in the unit of sub-networks is collected.

SOLUTION: The network traffic monitor system applied to a WAN is made up of a traffic monitor 5 whose branch cable connects to a point T between a TA 2 and a DSU 3 to monitor an Internet traffic and up of a monitor 6 that controls the traffic monitor 5 for start/stop of collection processing, sets a sub net mask to decide the collection unit and acquires traffic information in terms of an SNMP from the traffic monitor 5 as the collection result.



## LEGAL STATUS

[Date of request for examination] 31.10.1997

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-136237

(43) 公開日 平成11年(1999) 5月21日

(51) Int.Cl.<sup>6</sup>H 0 4 L 12/24  
12/26  
12/46  
12/28

識別記号

F I

H 0 4 L 11/08  
11/00

3 1 0 C

審査請求 有 請求項の数 6 O L (全 6 頁)

(21) 出願番号 特願平9-301068

(22) 出願日 平成9年(1997)10月31日

(71) 出願人 000004237

日本電気株式会社  
東京都港区芝五丁目7番1号

(72) 発明者 岩崎 順子

東京都港区芝五丁目7番1号 日本電気株  
式会社内

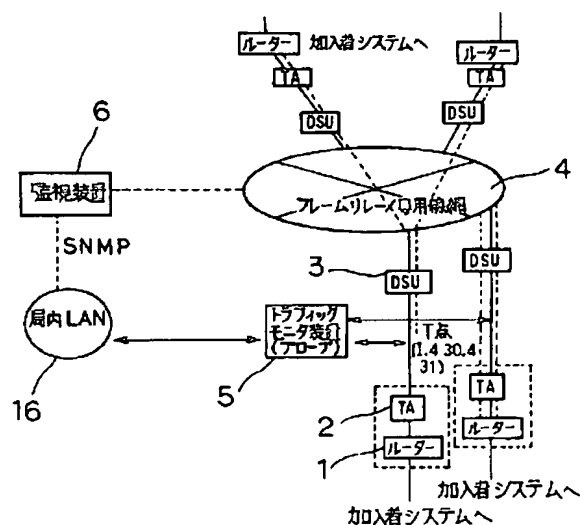
(74) 代理人 弁理士 若林 忠 (外4名)

(54) 【発明の名称】 ネットワークトラフィック監視システム

(57) 【要約】

【課題】 サブネットワーク単位の統計情報の収集を行い、WANに適したトラフィックの集計モニタができるネットワークトラフィック監視システムを提供する。

【解決手段】 WANに適用されるネットワークトラフィック監視システムであり、TA2-DSU3間のT点にて分岐ケーブルを接続し、インターネットトラフィックのモニタを行うトラフィックモニタ装置5と、トラフィックモニタ装置5に対し、集計処理の開始/停止などの制御、集計単位を定めるサブネットマスクの設定、及び、集計結果としてトラフィックモニタ装置5よりトラフィック情報をSNMPで取得する監視装置6より構成される。



## 【特許請求の範囲】

【請求項1】 加入者回線を収容するルーターと、該ルーターからネットワーク側へのインタフェースを変換する為のターミナルアダプタと、該ターミナルアダプタとインタフェースでつながる回線接続装置と、より高速な中継ルーターや交換機と伝送路より形成されるフレームリレー又は専用線網とを含む広域ネットワークに適用されるネットワークトラフィック監視システムであって、

前記ターミナルアダプタと前記回線接続装置との間の所定の点にて分岐ケーブルを接続し、前記ターミナルアダプタと前記回線接続装置との間の物理回線を流れるインターネットトラフィックのモニタを行うトラフィックモニタ装置と、

該トラフィックモニタ装置に対し、集計処理の開始及び停止の制御と、集計単位を定めるサブネットマスクの設定と、集計結果として前記トラフィックモニタ装置よりトラフィック情報をSNMPで取得する監視装置とから構成されるネットワークトラフィック監視システム。

【請求項2】 前記トラフィックモニタ装置と前記監視装置とは、制御情報及び集計情報のやりとりを行うマネジメント用のインタフェースで接続される請求項1記載のネットワークトラフィック監視システム。

【請求項3】 前記トラフィックモニタ装置は、前記ターミナルアダプタと前記回線接続装置との間の複数の物理回線を流れる双方向のインターネットトラフィックのモニタを行う請求項1記載のネットワークトラフィック監視システム。

【請求項4】 前記トラフィックモニタ装置は、前記ターミナルアダプタと前記回線接続装置間の前記フレームリレー又は専用線回線をモニタし、物理レイヤのフレームから、データリンクレイヤのフレーム単位に切り出しを行うインターフェース部と、受信したデータリンクレイヤのフレームをネットワークレイヤに解析及び集計するアナライザ部とを有する請求項1から請求項3のいずれか1項に記載のネットワークトラフィック監視システム。

【請求項5】 前記アナライザ部は、IPヘッダの送り元IPアドレスと送り先IPアドレスとのIPアドレス対毎の集計と、サブネットマスク設定による、送り元サブネットワークアドレスと送り先サブネットワークアドレスとのサブネットワークアドレス対間での統計情報の集計とを行うデータ集計処理部と、集計結果を記憶する共有メモリ部と、前記監視装置からの制御や前記集計結果の送信を行うSNMPエージェント部とを有する請求項4記載のネットワークトラフィック監視システム。

【請求項6】 前記データ集計処理部は、前記IPヘッダの送り元IPアドレスと送り先IPアド

レスとを読み出し、

前記監視装置により設定された前記サブネットマスクと、前記IPヘッダの送り元IPアドレスと送り先IPアドレスとの論理積をとることによって、前記送り元サブネットワークアドレスと前記送り先サブネットワークアドレスとを取得する手段を有する請求項5記載のネットワークトラフィック監視システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は広域ネットワークに適用されるネットワークトラフィック監視システムに関する。

【0002】

【従来の技術】従来、LANについて適用されたトラフィックモニタ装置について、送り元IPアドレスと送り先IPアドレスとを読み出し、送り元IPアドレスと送り先IPアドレスとの組合せ間で送信されたトラフィックに関する集計テーブルを作成し、情報収集していた。従来の技術の例は、特開平5-075621号公報、特開平6-318944号公報、特開平8-181711号公報及び特開平9-191327号公報に開示されている。

【0003】

【発明が解決しようとする課題】上述の方式を広域ネットワーク(WAN)にそのまま適用するとした場合、以下の問題点があった。

【0004】第1の問題点は、WANにおいて、収集される送り元IPアドレスと送り先IPアドレスとの組合せが膨大になるということである。

【0005】たとえば、n台のホストを含むWANでは、1集計時間内にIPホスト間通信の送り元IPアドレスと送り先IPアドレスとの組み合わせが、ネットワーク構成などによって、最悪n(n-1)通り発生する恐れがある。IPホスト間通信情報のみでは、大規模なWANについてのトラフィック傾向分析には、適当でない。

【0006】第2の問題点は、トラフィックモニタ装置において、送り元IPアドレスと送り先IPアドレスとの組み合わせを記憶する為のメモリの増加、テーブル検索にCPU処理時間が増大するということである。また、監視装置においても、取得するデータ量、解析/表示データ量が膨大になり処理性能が劣化する。

【0007】上記問題点を解決する為、本発明の目的は、サブネットワーク単位の統計情報の収集を行え、WANに適したトラフィックの集計モニタができるネットワークトラフィック監視システムを提供することにある。

【0008】

【課題を解決するための手段】本発明のネットワークトラフィック監視システムは、加入者回線を収容するルー

ターと、ルーターからネットワーク側へのインタフェースを変換する為のターミナルアダプタと、ターミナルアダプタと1インタフェースでつながる回線接続装置と、より高速な中継ルーターや交換機と伝送路より形成されるフレームリレー又は専用線網とを含む広域ネットワークに適用されるネットワークトラフィック監視システムであって、ターミナルアダプタと回線接続装置との間の所定の点にて分岐ケーブルを接続し、ターミナルアダプタと回線接続装置との間の物理回線を通るインターネットトラフィックのモニタを行うトラフィックモニタ装置と、トラフィックモニタ装置に対し、集計処理の開始及び停止の制御と、集計単位を定めるサブネットマスクの設定と、集計結果としてトラフィックモニタ装置よりトラフィック情報をSNMPで取得する監視装置とから構成される。

【0009】また、トラフィックモニタ装置と監視装置とは、制御情報及び集計情報のやりとりを行うマネジメント用のインタフェースで接続されてもよい。

【0010】また、トラフィックモニタ装置は、ターミナルアダプタと回線接続装置との間の複数の物理回線を通る双方向のインターネットトラフィックのモニタを行ってもよい。

【0011】また、トラフィックモニタ装置は、ターミナルアダプタ-回線接続装置間のフレームリレー又は専用線回線をモニタし、物理レイヤのフレームから、データリンクレイヤのフレーム単位に切り出しを行うインターフェース部と、受信したデータリンクレイヤのフレームをネットワークレイヤに解析及び集計するアナライザ部とを有してもよい。

【0012】また、アナライザ部は、IPヘッダの送り元IPアドレスと送り先IPアドレスとのIPアドレス対毎の集計と、サブネットマスク設定による、送り元サブネットワークアドレスと送り先サブネットワークアドレスとのサブネットワークアドレス対間での統計情報の集計とを行うデータ集計処理部と、集計結果を記憶する共有メモリ部と、監視装置からの制御や集計結果の送信を行うSNMPエージェント部とを有してもよい。

【0013】また、データ集計処理部は、IPヘッダの送り元IPアドレスと送り先IPアドレスとを読み出し、監視装置により設定されたサブネットマスクと、IPヘッダの送り元IPアドレスと送り先IPアドレスとの論理積をとることによって、送り元サブネットワークアドレスと送り先サブネットワークアドレスとを取得する手段を有してもよい。

【0014】従って、送り元IPアドレス/送り先IPアドレス対のデータを収集する時にデータをまとめる単位を設定することにより、ポイント-ポイント間の統計情報ではなく、サブネットワーク単位のトラフィック情報を集約して集計することができ、大規模なWANのインターネットトラフィックのトレンド解析を実施するこ

とができる。

【0015】また、IPパケットの集計において送り元IPアドレス/送り先IPアドレスをそれぞれネットマスクすることにより、ポイント-ポイント間の統計情報ではなく、サブネットワーク単位の統計情報の収集を行い、WANに適したトラフィックの集計モニタができる。

【0016】

【発明の実施の形態】次に、図を用いて、主として本発明の実施の形態の構成を説明する。

【0017】本発明は、図1に示すネットワーク、すなわち加入者回線を収容するルーター1と、ルーターからネットワーク側へインタフェースを変換するターミナルアダプタ(TA)2、TAと1インタフェースでつながる回線接続装置(DSU)3、及び、より高速な中継ルーターや交換機と伝送路より形成されるフレームリレー/専用線網4を含むWANに適用されるネットワークトラフィック監視システムであり、TA-DSU間のT点にて分岐ケーブルを接続し、インターネットトラフィックのモニタを行うトラフィックモニタ装置5と、トラフィックモニタ装置5に対し、集計処理の開始/停止などの制御、集計単位を定めるサブネットマスクの設定、及び、集計結果としてトラフィックモニタ装置5よりトラフィック情報をSNMPで取得する監視装置6より構成される。

【0018】また、トラフィックモニタ装置5と監視装置6は、制御情報や集計情報のやりとりを行うマネジメント用のインタフェースで接続される。

【0019】次に、図2を用いてトラフィックモニタ装置5の構成を説明する。

【0020】トラフィックモニタ装置5は、TA-DSU間のフレームリレー/専用線回線をモニタし、物理レイヤのフレームから、データリンクレイヤのフレーム(図3に例示されるようなQ.922フレーム、または、PPPのフレーム)単位に切り出しを行うインターフェース部7、受信したデータリンクレイヤのフレームをネットワークレイヤに解析/集計するアナライザ部8を持ち、アナライザ部8は、さらに、機能上、送り元IPアドレスと送り先IPアドレスとのIPアドレス対毎の集計や、サブネットマスク設定による、送り元サブネットワークアドレスと送り先サブネットワークアドレスとのサブネットワークアドレス対間での統計情報の集計を行うデータ集計処理部9、集計結果を記憶する共有メモリ部10、監視装置6からの制御や/集計結果の送信を行うSNMPエージェント部11などを持つ。

【0021】また、トラフィックモニタ装置5は、複数の物理回線について双方向のトラフィックのモニタができるように実現することもできる。

【0022】次に、本発明の実施の形態の動作について説明する。

【0023】本発明のトラフィック監視システムでは、送り元IPアドレスと送り先IPアドレスとのIPアドレス対のデータを収集する時にデータをまとめる単位を設定することができる。

【0024】本発明の実施の形態の動作を順番に説明する。

【0025】1. 監視装置6から、トラフィックモニタ装置5に対し収集開始要求時、サブネットワーク間のトラフィック量を取得する為、IPアドレスについてマスクするビットを設定する。

【0026】ここで、IPアドレスに設定するマスクは、(255.255.255.0)、(255.255.0.0)、(255.0.0.0)などの単位、またはビット単位にマスクビットの設定が行える。

【0027】2. トラフィックモニタ装置5は、マスク値を受信すると、アナライザ部8に記憶するとともに、インタフェース部7を介し、トラフィックデータの収集を開始する。

【0028】3. トラフィックモニタ装置5は、インタフェース部7を介し、フレームリレー/専用線回線上に流れる物理レイヤのフレームをモニタし、開始/終了フラグ位置より、データリンクレイヤのフレーム(特にフレームリレーについては図3に示されるようなQ、922フレーム。専用線に関してはPPPのフレーム)単位に切り出しを行った後、データをアナライザ部8へ転送を行う。

【0029】4. アナライザ部8は、データリンクレイヤのフレームを解析し、情報フィールドの値からレイヤ3/4/アプリケーションレベルのインターネットトラフィックの解析を行う。

【0030】すなわち、フレームリレー回線については、データリンクレイヤのQ、922フレームについてPVCの識別子(DLCI)、情報フィールドの値(NLPID等)よりネットワーク層プロトコルの識別を行い、IPデータであればヘッダ情報より、送り元IPアドレスと送り先IPアドレスとを読みとる。

【0031】5. サブネットマスクが設定されていない場合、送り元IPアドレスと送り先IPアドレスとの組み合わせ毎に集計テーブルを作成し、送り元IPアドレスと送り先IPアドレスとのIPアドレス対の統計情報を収集する。

【0032】ここで、集計テーブルの中身の例としては、伝送方向、PVC識別子(DLCI)、プロトコル種別、送り元IPアドレスと送り先IPアドレス、収集開始時間、オクテット数、パケット数などを集計単位として生成する場合がある。

【0033】6. サブネットマスクが設定されている場合、送り元IPアドレスと送り先IPアドレスをそれぞれネットマスクすることにより集計単位をサブネット単位に集約し、集計結果を集計テーブルとして作成する。

【0034】7. 集計テーブルはトラフィックモニタ装置内の共有メモリ部10に一時記憶され、SNMPエージェント部11の機能により、監視装置6へ集計データの送信を行う。

【0035】8. 監視装置6は、サブネットワーク間のトラフィック統計情報として、解析表示を行う。

【0036】以上の動作によりポイント-ポイント間の統計情報のみではなく、サブネットワークとサブネットワークとの間での統計情報の収集が行える。

10 【0037】次に図4、図5を参照してサブネットワーク単位の集計処理について説明する。

【0038】図4に示すように加入者ルータのユーザー側に、複数のIPホストが接続されているサブネットワークがあり、IPアドレスA.A.A.A.とIPアドレスB.B.B.B.のホスト間、及びIPアドレスA.A.A.CとIPアドレスB.B.B.Dのホスト間で通信データが、送られているものとする。

【0039】一例としてネットマスク値(255.255.255.0)によって、IPアドレスをネットマスクした場合の収集フレームとアドレス対テーブルの関係を図5に示す。

【0040】収集したIPデータグラム内の送り元IPアドレス/送り先IPアドレス対について、(A.A.A.A.)→(B.B.B.B.)n個と(A.A.A.C)→(B.B.B.D)m個とは、ネットマスクされると、同じ送り元/送り先サブネットワークアドレス対収集テーブル(A.A.A.0)→(B.B.B.0)に集計される。(n+m個)また、実施例として必要時のみ送り元IPアドレスと送り先IPアドレスとの間のトラフィック計測を併用することにより、詳細トラフィック分析を実施することもできる。

30 【0041】

【発明の効果】以上説明したように本発明においては、以下に記載するような効果を持つ。

【0042】本発明のネットワークトラフィック監視システムでは、送り元IPアドレス/送り先IPアドレス対のデータを収集する時にデータをまとめる単位を設定することにより、ポイント-ポイント間の統計情報ではなく、サブネットワーク単位のトラフィック情報を集約して集計することができ、大規模なWANのインターネットトラフィックのトレンド解析を実施することができるといふ効果がある。

【0043】また、IPパケットの集計において送り元IPアドレス/送り先IPアドレスをそれぞれネットマスクすることにより、ポイント-ポイント間の統計情報ではなく、サブネットワーク単位の統計情報の収集を行え、WANに適したトラフィックの集計モニタができるという効果がある。

【0044】また、トラフィックモニタ装置及び監視装置両方のメモリ量の削減と性能向上が行えるという効果がある。

## 【図面の簡単な説明】

【図1】本発明の実施の形態が適用される広域ネットワーク（WAN）を示す図である。

【図2】本発明の実施の形態のトラフィックモニタ装置の構成図である。

【図3】データリンク層フレーム例を示す図である。

【図4】加入者ルータのユーザー側に、複数のIPホストが接続されているサブネットワークを示す図である。

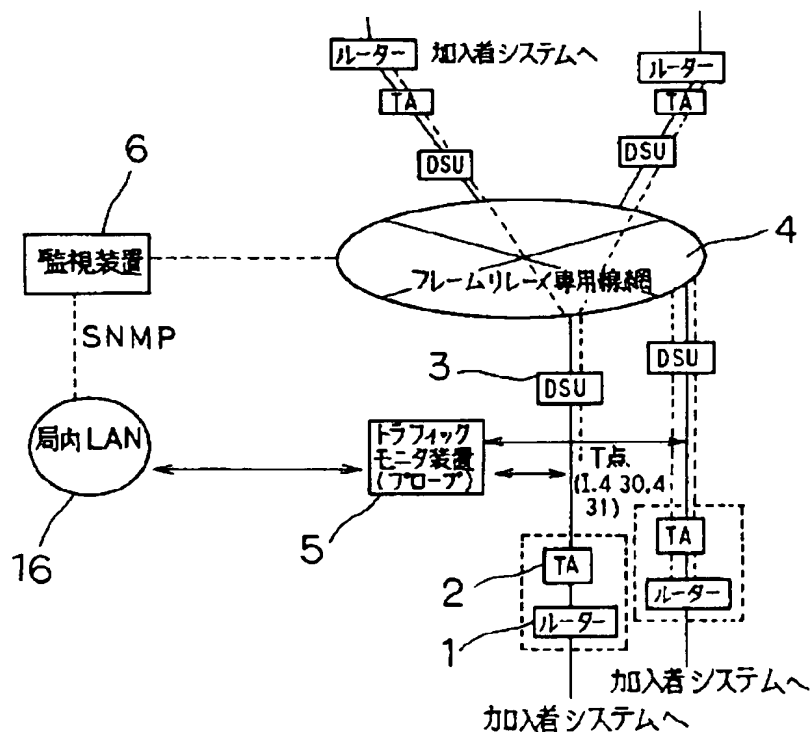
【図5】ネットマスク値（255.255.255.0）によって、IPアドレスをネットマスクした場合の収集フレームとアドレス対テーブルの関係を示す図である。

## 【符号の説明】

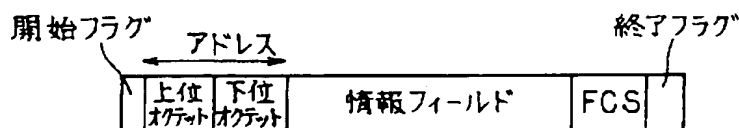
- 1 ルーター
- 2 ターミナルアダプタ（TA）
- 3 回線接続装置（DSU）
- 4 フレームリレー／専用線網

- \* 5 トラフィックモニタ装置
- 6 監視装置
- 7 インターフェース部
- 8 アナライザ部
- 9 データ集計処理部
- 10 共有メモリ部
- 11 SNMPエージェント部
- 12 デバイスドライバ
- 13 IFモジュール
- 14 モニタCPU部
- 15 DPM
- 16 局内LAN
- 17 広域ネットワーク（WAN）
- 18 サブネットワーク
- 19 IPホスト
- \* 20 モニタ点

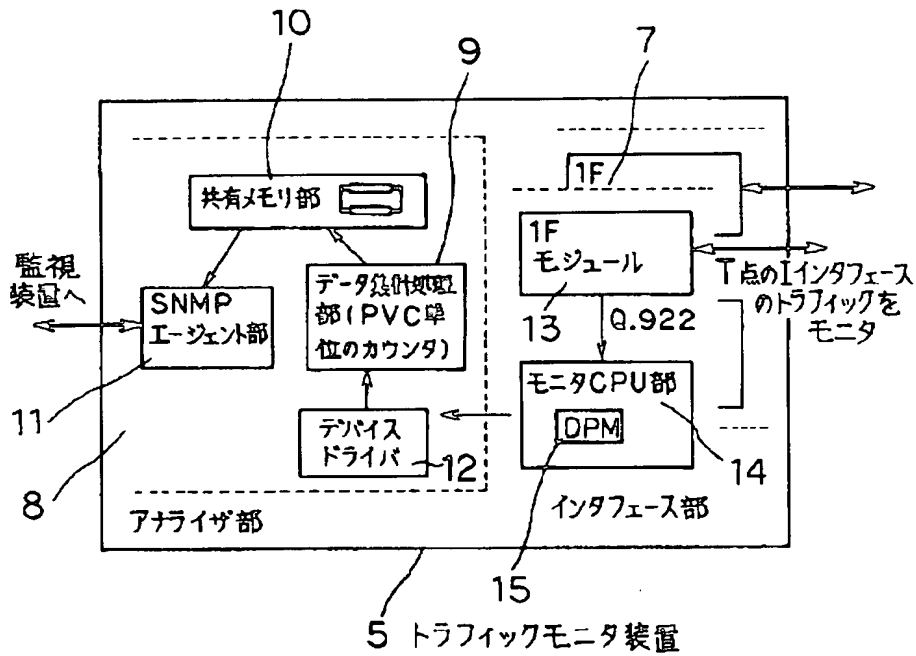
【図1】



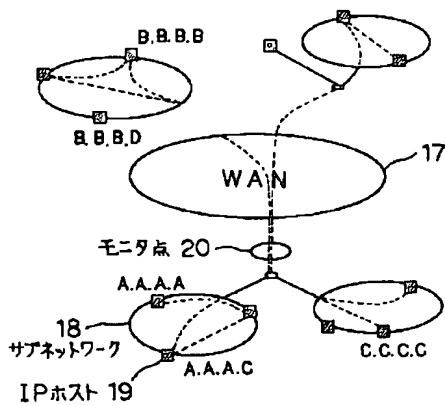
【図3】



【図2】



【図4】



【図5】

